(12) UK Patent Application (19) GB (11) 2 265 482 (13) A

(43) Date of A publication 29.09.1993

(21) Application No 9206851.9

(22) Date of filing 28.03.1992

(51) INT CL[5]
B60R 25/10

(52) UK CL (Edition L)
G4H HTG H1A H13D H14A H14B H14D
U1S S1820 S2188

(56) Documents cited
GB 2257552 A GB 2254461 A

(58) Field of search
UK CL (Edition L) G4H HTG
INT CL[5] B60R, G07C

(71) Applicant
Pektron Limited

(Incorporated in the United Kingdom)

Alfreton Road, Breadsall, Derby, DE2 4AP, United Kingdom

(72) Inventor
Robert John Tibbetts

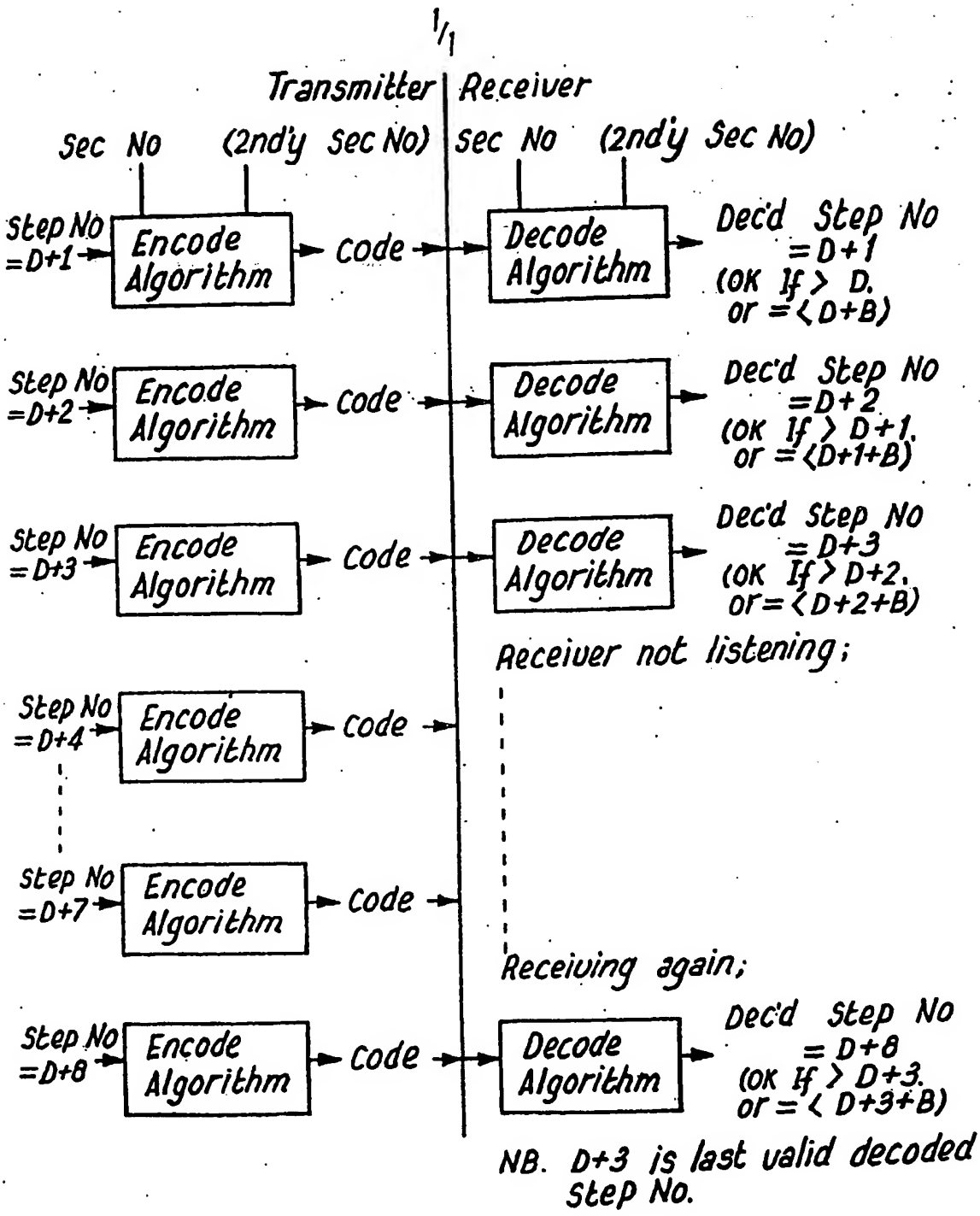
(74) Agent and/or Address for Service
Swindell & Pearson
48 Friar Gate, Derby, DE1 1GY, United Kingdom

(54) Security system data transmission

(57) A motor vehicle alarm system has a radio transmitter convenient for carrying by the driver of the vehicle, and a radio receiver suitably located inside the vehicle. The transmitter can be operated remotely to transmit a numerical rolling or dynamic code whereby a different code is transmitted each time. Such a code is determined by the use of a preselected security number and a randomly selected step number, the latter being altered in each transmission. The transmitter uses the security and step numbers in an algorithm, and the receiver, provided with the security number, can use the latter and the code in a reverse algorithm in order to reproduce the step number. Comparison with a previously stored step number is then made by the receiver to prevent a response to an unauthorised transmission.

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

The claims were filed later than the filing data within the period prescribed by Rule 25(1) of the Patents Rules 1990..


Transmitter
Receiver
Sec No
(2nd'y Sec No)
Sec No
(2nd'y Sec No)
Step No =D+1
Encode Algorithm
code
Decode Algorithm
Dec'd Step No =D+1 (OK If > D. or =< D+B)
Step No =D+2
Encode Algorithm
code
Decode Algorithm
Dec'd Step No =D+2 (OK If > D+1. or =< D+1+B)
Step No =D+3
Encode Algorithm
code
Decode Algorithm
Dec'd Step No =D+3 (OK If > D+2. or =< D+2+B)
Receiver not listening;
Step No =D+4
Encode Algorithm
code
Step No =D+7
Encode Algorithm
code
Receiving again;
Step No =D+8
Encode Algorithm
code
Decode Algorithm
Dec'd Step No =D+8 (OK If > D+3. or =< D+3+B)
NB. D+3 is last valid decoded Step No.

Improvements in Data Transmission

This invention relates to an arrangement for and method of transmitting data, particularly but not exclusively concerned with the secure transmission of numerical codes, for example for remote control of a motor vehicle burglar alarm system.

When transmitting data, it is sometimes necessary for security reasons for the transmitter to send a special code, such that the receiver will only accept the data if the receiver also gets the correct code. Such a code can be static, i.e. a fixed code. A weakness of this, particularly if it is possible for an unauthorised third party to tap into the transmission medium, is that the third party can listen to the transmitted code, and then re-transmit the code to access the receiver. This is a particular problem with radio systems. A rolling or dynamic code system can alternatively be used, whereby a different code is sent each time. However, present rolling or dynamic code systems have not proved sufficiently successful in preventing an unauthorised third party from identifying acceptable codes and thereby gaining access to the receiver.

Reference is made hereinafter to the code transmission by way of "wave energy". The term is to be construed as embracing transmission by way of any of radio waves, infrared waves, ultrasonics and other like energy.

According to the present invention there is provided a data transmission arrangement comprising means for transmitting a code by way of wave energy, the transmitting means being provided with means for storing a preselected first parameter, means for generating a second parameter, and means for producing the code for transmission from the first and second parameters, and receiving means, the latter being provided with means for storing the preselected first parameter, means for receiving the code transmitted by the transmitting means, means for reproducing the second parameter from the code and the first parameter, means for comparing the reproduced second parameter with at least one parameter previously reproduced and accepted, and means for accepting the second parameter and thereby responding to the transmitted code only after the reproduced second parameter is confirmed to have a predetermined relation to said at least one previously reproduced parameter.

Preferably the transmitting means is adapted to transmit a numerical code and each of the first and second parameters is a number. The preselected first number is preferably randomly preselected.

Preferably also the parameter with which the second number is compared is a previously reproduced second number which was accepted by the receiving means

after comparison, means being provided for storing the previously accepted second number for subsequent comparison purposes. The comparison means includes means for checking that the reproduced second number is greater than the stored second number, and preferably also includes means for checking that the reproduced second number is not greater than the stored second number by a preselected amount.

The second number generating means may be adapted to increment the second number, for example by one, each time a code is transmitted. Also the second number generating means may be initially provided with a randomly selected second number, and means may be provided in each of the transmitting means and the receiving means to store this initial randomly selected second number.

The transmitting means may be provided with means for storing a further preselected number which is required to be used by the code producing means, the receiving means being provided with means for storing the further preselected number which is required to be used by the means reproducing the second number. Further, the transmitting means may be adapted to randomly generate the second preselected number and may also be adapted to alter the further number and transmit same, the receiving means being adapted to receive the

transmitted second number and store same.

The present invention also provides a method of transmitting data by way of wave energy, comprising the steps of producing a code for transmission from transmitting means by utilising a preselected first parameter and a second parameter generated by the transmitting means, transmitting the produced code, receiving the transmitted code in transmitting means and therein reproducing the second parameter from the code and the preselected first parameter available to the receiving means, comparing the reproduced second parameter with at least one parameter previously reproduced and accepted by the receiving means, and enabling the receiving means to accept the second parameter and thereby respond to the transmitted code, only after confirmation that the reproduced second parameter has a predetermined relation to said at least one previously reproduced parameter.

Preferably the method comprises transmission of a numerical code, and the code may be transmitted in the form of a radio signal.

Preferably also the comparison includes checking that the reproduced second parameter is greater than the stored second parameter, and further may include checking that the reproduced second parameter is not greater

than the stored second parameter by a preselected amount.

An embodiment of the present invention will now be described by way of example only with reference to the accompanying drawing which is a diagrammatic representation of the operation of a data transmission arrangement according to the invention.

A motor vehicle burglar alarm system has a radio transmitter in the form of a relatively small device convenient for carrying by the driver of the vehicle, for example on a keyring, and a radio receiver suitably located inside the vehicle. Appropriate operation of a switch on the transmitter transmits a radio signal in the form of a code which can be detected by the receiver, with the result that the latter arms an alarm system within the vehicle. The latter may comprise sensors which can detect when there is unauthorised entry to the vehicle, at which time any suitable warning system, for example a siren, can be activated. Subsequent operation of the same switch on the transmitter can then disarm the alarm system.

The alarm system is designed to utilise a rolling or dynamic code system, whereby a different code is transmitted each time by the transmitter. The

transmitter utilises suitable electrical circuitry to enable storing of a preselected first or 'security' number, and also to store initially a second or 'step' number. The security number is initially randomly chosen, and the receiver is also adapted to store the same security number. The initial step number is also randomly chosen and again the receiver is adapted to store the same number. In order to produce a required numerical code for transmission, the transmitter uses the security and step numbers in an algorithm. Each time a code is transmitted, the transmitter increments a counter therein by one, in order to generate a new step number for use in the next transmission.

When the transmitted code is received by the receiver, the latter uses the security number and the code in an algorithm, which is the reverse of the transmitter algorithm, in order to reproduce the step number. The reproduced step number is then compared with a previously stored step number to ensure that the reproduced step number is greater than the stored step number, and also checks that the reproduced step number is not greater than the stored step number by a certain amount. The former checking ensures that no previously sent code is accepted by the receiver. The latter checking produces a band of acceptable codes. The greater this band, the more times the transmitter can send codes when

the receiver is not listening. It will be appreciated that, after accepting an initial code, the receiver will each time store the most recently accepted step number which will be used for comparison with the step number reproduced from the next code which is transmitted and received.

It may be preferred to utilise a secondary security number in order to avoid the requirement of a large range of security numbers. Such a secondary security number need not be a fixed number but would have to be stored, when appropriate, by both the transmitter and the receiver. The secondary security number would be utilised in producing the code to be transmitted, and could be a number randomly generated by the transmitter and sent to the receiver. With this arrangement, the secondary security number could be changed regularly. Alternatively the secondary security number could be chosen to be the initial step number.

In the case of a system where the receiver is not always listening to the transmitter, such that a number of codes could be sent without being accepted, the receiver should be able to accept the next code that is sent after it has started to listen again. In the radio system, for example, the transmitter may sometimes be operated out of range.

In the drawing, the first security number is identified as 'Sec. No.', the initial step number is identified by D, and the secondary security number (which is not in this case the same as the initial step number) is identified as '2nd'y Sec. No.' The diagrammatic representation shows the step number increasing in increments of one. The band of acceptable codes is identified by B, and the representation shows that the transmitter can send B-1 codes with the receiver not listening, and still be aligned when the next code is received.

In normal operation, pressing of the transmitter switch sends the next code in the rolling code sequence. This is received and decoded by the receiver in the vehicle, and if in the acceptable band of codes, the code is acted upon by the receiver.

The security number, the initial step number, and the secondary security number could be stored in the transmitter and receiver by any of a variety of methods. For example, the numbers could be physically embedded by way of links or drilled holes in a printed circuit board, or the numbers could be held in non-volatile memory circuitry. It may be possible to set up the transmitter and receiver with the numbers separately. However, it may be desirable in certain situations for the transmitter to send information relating to these

numbers to the receiver in a special "start up signal". If required, the receiver could be arranged to only accept this information when the receiver is in a special learn mode. Alternatively, the receiver could be arranged to only accept a new security number in the learn mode, but to accept a new secondary security number at any time.

The number of transmitter - receiver pairs having the same security number should be kept to a minimum, thus minimising the chances of a transmitter accessing the wrong receiver.

The arrangement described above obviates or mitigates the likelihood of an unauthorised third party finding a code which is acceptable to the receiver by listening to a transmitted code, and therefore provides increased transmission security.

The greater the number of step numbers, the greater the number of different codes, and thus the more difficult it is for a third party to find an acceptable code. If the step numbers were to start at zero then a third party might know not to bother with higher step numbers, on the basis that the amount of codes ever likely to be sent is much less than the total available. For this reason, the initial step number is randomly

chosen as referred to above within the step number range. For the same reasons, the security number is randomly chosen. An optional check can be carried out to avoid repeating numbers.

Where a third party is able to listen to several consecutive codes, then attempts to compute the next code using a trial and error method, whereby different security numbers are tried until the captured sequence of codes can be recreated, then the time taken to find the correct security number will obviously be longer the greater the range of security numbers. However, it may not be desirable to have a large amount of security numbers for various reasons, for example where the security number is established by hardware switches, a large number of switches would be expensive, and where the security number may need to be written and quoted, too larger a number might be cumbersome. For this reason, the secondary security number can be used.

Another problem which can occur involves a third party transmitting a stream of different codes in order to happen upon a correct one. For this reason, the time for a code stream generator to find an acceptable code should be very long. This time can be increased by reducing the rate at which the receiver will listen to codes, for example by having a minimum time from

reception of one code before listening for another.

Various modifications may be made without departing from the invention. For example, the code may be transmitted by infrared, ultrasonics, or any other suitable form of wave energy. Also different switches for arming, disarming and other formations could be used on the transmitter.

Whilst endeavouring in the foregoing Specification to draw attention to those features of the invention believed to be of particular importance it should be understood that the Applicant claims protection in respect of any patentable feature or combination of features hereinbefore referred to and/or shown in the drawings whether or not particular emphasis has been placed thereon.

Claims:-

1. A data transmission arrangement comprising means for transmitting a code by way of wave energy, the transmitting means being provided with means for storing a preselected first parameter, means for generating a second parameter, and means for producing the code for transmission from the first and second parameters, and receiving means, the latter being provided with means for storing the preselected first parameter, means for receiving the code transmitted by the transmitting means, means for reproducing the second parameter from the code and the first parameter, means for comparing the reproduced second parameter with at least one parameter previously reproduced and accepted, and means for accepting the second parameter and thereby responding to the transmitted code only after the reproduced second parameter is confirmed to have a predetermined relation to said at least one previously reproduced parameter.

2. An arrangement according to Claim 1, wherein the preselected first parameter is randomly preselected.

3. An arrangement according to Claim 1 or 2, wherein the transmitting means is adapted to transmit a

numerical code and each of the first and second parameters is a number.

4. An arrangement according to Claim 3, wherein the parameter with which the second number is compared is a previously reproduced second number which was accepted by the receiving means after comparison, means being provided for storing the previously accepted second number for subsequent comparison purposes.

5. An arrangement according to Claim 4, wherein the comparison means includes means for checking that the reproduced second number is greater than the stored second number.

6. An arrangement according to Claim 4 or 5, wherein the comparison means includes means for checking that the reproduced second number is not greater than the stored second number by a preselected amount.

7. An arrangement according to any of Claims 3 to 6, wherein the second number generating means is adapted to increment the second number each time a code is transmitted.

8. An arrangement according to Claim 7, wherein the second number generating means is adapted to increment

the second number by one.

9. An arrangement according to any of Claims 3 to 8, wherein the second number generating means is initially provided with a randomly selected second number.

10. An arrangement according to Claim 9, wherein means is provided in each of the transmitting means and the receiving means to store the initial randomly selected second number.

11. An arrangement according to any of Claims 3 to 10, wherein the transmitting means is provided with means for storing a further preselected number which is required to be used by the code producing means, the receiving means being provided with means for storing the further preselected number which is required to be used by the means reproducing the second number.

12. An arrangement according to Claim 11, wherein the transmitting means is adapted to randomly generate the further preselected number.

13. An arrangement according to Claim 12, wherein the transmitting means is adapted to alter the further number and transmit same.

14. An arrangement according to Claim 12 or 13, wherein the receiving means is adapted to receive the transmitted further number and store same.

15. A motor vehicle alarm system comprising a data transmission arrangement according to any of the preceding Claims.

16. A method of transmitting data by way of wave energy, comprising the steps of producing a code for transmission from transmitting means by utilising a preselected first parameter and a second parameter generated by the transmitting means, transmitting the produced code, receiving the transmitted code in transmitting means and therein reproducing the second parameter from the code and the preselected first parameter available to the receiving means, comparing the reproduced second parameter with at least one parameter previously reproduced and accepted by the receiving means, and enabling the receiving means to accept the second parameter and thereby respond to the transmitted code, only after confirmation that the reproduced second parameter has a predetermined relation to said at least one previously reproduced parameter.

17. A method according to Claim 16, wherein transmission is by way of a numerical code.

18. A method according to Claim 16 or 17, wherein the code is transmitted in the form of a radio signal.

19. A method according to any of Claims 16 to 18, wherein the comparison includes checking that the reproduced second parameter is greater than the stored second parameter.

20. A method according to Claim 18, wherein the comparison includes checking that the reproduced second parameter is not greater than the stored second parameter by a preselected amount.

21. A data transmission arrangement substantially as hereinbefore described with reference to the accompanying drawings.

22. A method of transmitting data substantially as hereinbefore described with reference to the accompanying drawings.

23. Any novel subject matter or combination including novel subject matter disclosed, whether or not within the scope of or relating to the same invention as any of the preceding Claims.

Patents Act 1977
Examiner's report to the Comptroller under Section 17 (The Search Report)

Application number
GB 9206851.9

Relevant Technical fields

(i) UK Cl (Edition L) G4H (HTG)

(ii) Int Cl (Edition 5) B60R, G07C

Search Examiner
M J DAVIS

Databases (see over)

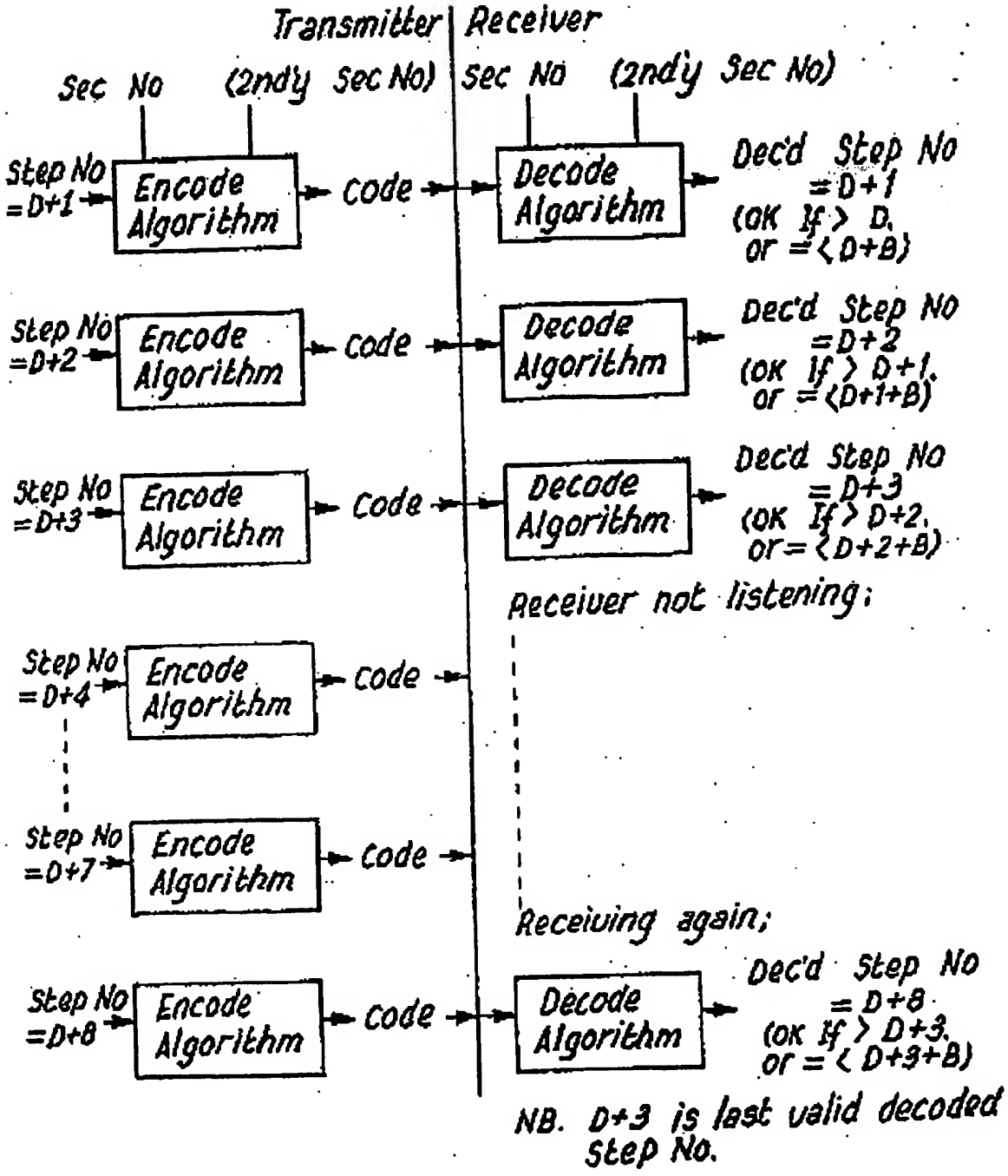
(i) UK Patent Office

(ii)

Date of Search
11 MAY 1993

Documents considered relevant following a search in respect of claims 1-22

Category (see over)	Identity of document and relevant passages	Relevant to claim(s)
X,E	GB 2257552 A (TRW SIPEA), whole document, especially pages 9-10	1,16 at least
X,E	GB 2254461 A (ALPS ELECTRIC), whole document	1,16 at least


Transmitter
Receiver
Sec No
(2nd'y Sec No)
Sec No
(2nd'y Sec No)
Step No = D+1
Encode Algorithm
code
Decode Algorithm
Dec'd Step No = D+1 (OK If > D, or = < D+B)
Step No = D+2
Encode Algorithm
code
Decode Algorithm
Dec'd Step No = D+2 (OK If > D+1, or = < D+1+B)
Step No = D+3
Encode Algorithm
Code
Decode Algorithm
Dec'd Step No = D+3 (OK If > D+2, or = < D+2+B)
Receiver not listening;
Step No = D+4
Encode Algorithm
code
Step No = D+7
Encode Algorithm
code
Receiving again;
Step No = D+8
Encode Algorithm
code
Decode Algorithm
Dec'd Step No = D+8 (OK If > D+3, or = < D+3+B)
NB. D+3 is last valid decoded Step No.